User Manual

Date: 2015-05-14 - Version 1.2

Table of contents

Author....3
Naming....3
Server....3
  Description of base setup....4
  Backup....4
User resources....5
  Disk space....5
  Processes and RAM....5
  Account lock....5
Servername / Network addresses....6
  IPV4....6
  IPV6....6
  Connectivity....6
System identification / Certificates....7
  DNSSEC....7
  SSH-Fingerprint....7
  SSL-Fingerprint....8
  PGP - Public Key....9
  S/MIME - Public Key....10
Authentication and access....11
  SSH....11
    Password....11
    Public Key....11
    Yubikey....12
    Two-Factor-Login (forced)....13
    OTP / OPIE Auth....14
    limited access / censored internet....15
Software and services....17
  OS....17
  Installation of additional packages....17
  Firewall....17
  Mailsystem....18
    Postfix....18
    Anti-Spam / Anti-Virus....18
    Dovecot - Receive mail....19
    Zarafa - Groupware....19
    ActiveSync – Push-Services....21
  Owncloud....21
  Homepage / PHP....23
  MySQL-Database....23
  Tor and anonymous surfing....23
Support and help....23
Link collection....24
Disclaimer / Misc....24

Author

Contact private:
Sebastian Krajenski
Im Gehren 24/1
73732 Esslingen
Germany
Tel: +49-162-8741288 (SMS possible / only for emergencies like: “server down”)
E-Mail: postmaster@ freeshell.de

Contact business:
mars solutions GmbH
Robert-Bosch-Str. 8
73037 Goeppingen
Germany
Tel: +49-7161-6549250 (Mon-Fri)
E-Mail: sebastian.krajenski@ mars-solutions.de

Business proposals welcome. I'm a certified RHCE7, LPIC-3 (security) with 19 years of Linux experience in general.

Naming

The project is called “**freeshell.de**”, like the homepage and main domain name. The old name of “Nic.Nac.Project” is not in use anymore.

Server

The momentarily used system is a Intel-based 64-bit-system with the following specs:

- Processor i3-3220T with 2.8 GHz (4 Cores)
- 8.0 GB RAM
- 2x 500GB WD SATA HDD

Description of base setup

The setup as such is a single-server system. Regarding the HDDs a software RAID1 is used. Both HDD get monitored using “smartd”. Daily tests (“short-test”) as well as weekly tests (“long-test”) assure that possible SMART-Errors are detected as quickly as possible.

Nameserver situation of “freeshell.de”:
NS1: ns1.nic-nac-project.de, NS2: ns2.nic-nac-project.de

In detail:
ns1.nic-nac-project.de = freeshell.de (the server itself, the MASTER-DNS)
ns2.nic-nac-project.de = 50.30.38.228 (a vServer in USA , exclusively used as SLAVE-DNS)

The old legacy-domain nic-nac-project.de itself is served from those nameservers:
nsa5.schlundtech.de
nsb5.schlundtech.de
nsc5.schlundtech.de
nsd5.schlundtech.de

A backup MX-record doesn't exist at the moment, but is planned.

The hardware- and software-situation as well as the DNS-setup is permanent “work-in-progress”. There may be regular updates and improvements.

Backup

The system is saved to another data centre on a daily basis using “duplicity”. The data is gpg-encrypted. The command I'm using is:

 # duplicity incremental --encrypt-key <Key-ID> --full-if-older-than 30D -v3 / file:///backup
365 restore-points are saved at the moment. In case you need a restore, please always name the exact and absolute path as well as a best-estimate regarding the date the data was still intact.

User resources

Disk space

There are different quotas for you depending on what services we're talking about:

- Linux $HOME-directory incl. Maildir/ → 256MB
- MySQL database → 256MB
- Zarafa-Groupware mailbox→ 512MB
- OwnCloud service → 1024MB

Processes and RAM

Here is an overview on what resources to expect on the shell:

$ ulimit -a

```
data seg size           (kbytes, -d) 256000
file size               (blocks, -f) unlimited
pending signals                 (-i) 63359
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) 256000
open files                      (-n) 1024
pipe size            (512 bytes, -p) 8
POSIX message queues     (bytes, -q) 819200
stack size              (kbytes, -s) 8192
cpu time               (seconds, -t) 300
max user processes              (-u) 50
virtual memory          (kbytes, -v) 512000
file locks                      (-x) unlimited
```

Account lock

Basically this is covered in the "terms and conditions".
For short: Misuse of any kind as well as illegal content will lead to deletion as well as account lock.
I don't spy into your files, but there is a automated process using commercial anti-virus-software to find virus- and trojaned files. They get automatically deleted.
For optimal privacy I recommend you to use TrueCrypt, gpg or similar software.

Servername / Network addresses

IPV4

Assigned: 94.247.40.144 – 94.247.40.159

In use:
94.247.40.145 – Default-GW
94.247.40.147 – DNS-Name: ssh.freeshell.de
94.247.40.152 – DNS-Name: zarafa.freeshell.de
94.247.40.153 – "DNS2TCP"-address (see -> "censored internet")
94.247.40.155 – DNS-Name: secure.freeshell.de
94.247.40.156 – DNS-Name: **freeshell.de** (IPV4 main address)

IPV6

Assigned: 2a01:360:106::2 / 48

In use:
2a01:360:106::2 – DNS-Name: **freeshell.de** (IPV6 main IP of the server)

Connectivity

The server is connected by a 100MBit/s-Link to the internet.
In case of a D(D)oS-attack the system automatically gets disconnected from the infrastructure.
Likewise it is automatically connected back when the attack stops.

System identification / Certificates

DNSSEC

The DNS of the main domain “freeshell.de” is secured with DNSSEC.
I recommend the following URLs to check out the zone:
URL: http://dnssec-debugger.verisignlabs.com/freeshell.de

URL: https://www.dnssec-validator.cz/
There you'll find a neat **Browser-Plugin** that checks for a couple of things. The availability of DNSSEC for that domain (key symbol), as well as the validity of TLSA-entries.

At the moment I maintain TLSA-entries for the following names/services:

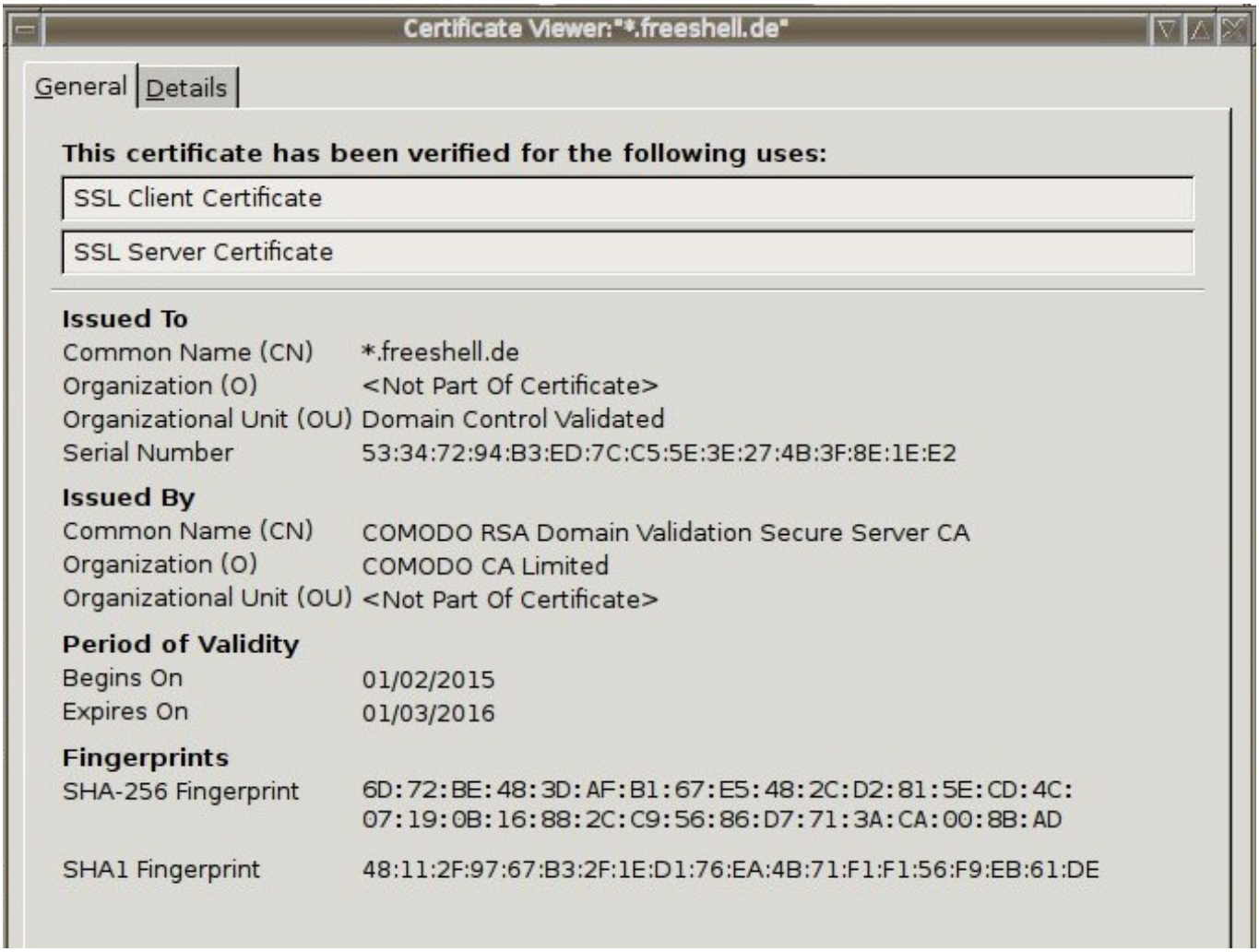
_443._tcp.freeshell.de.
_443._tcp.www.freeshell.de.
_443._tcp.secure.freeshell.de.
_25._tcp.freeshell.de. → "postfix" is configured DANE-compatible here.
_465._tcp.freeshell.de.
_587._tcp.freeshell.de.

SSH-Fingerprint

SSH Fingerprint freeshell.de (RSA): **0c:39:00:1a:11:4a:1c:09:4d:7c:06:6e:19:15:7a:c7**
SSH Fingerprint freeshell.de (ED25519): **92:61:df:85:1b:07:1b:6a:04:34:96:be:49:cf:9e:f0**

Hint: In case of "untrusted" or mobile situations like Internet Cafe, hotel etc. I deeply recommend to print out the fingerprints on a piece of paper and carry them with you. You prevent "man-in-the-middle" attacks this way.

SSL-Fingerprint



Copy-Paste-variant of the SHA-256-Fingerprint:
6D:72:BE:48:3D:AF:B1:67:E5:48:2C:D2:81:5E:CD:4C:07:19:0B:16:88:2C:C9:56:86:D7:71:3A:CA:00:8B:AD

The webserver also uses “**certificate pinning**”. Modern browsers may know this way if the certificate delivered is the right one. This technique relies on "trusted first visit" of course.

Technical background info: https://tools.ietf.org/html/draft-ietf-websec-key-pinning-21
Implementation hints: https://developer.mozilla.org/en-US/docs/Web/Security/Public_Key_Pinning

PGP - Public Key

This is my public key for safe email communication. My address: sk@ freeshell.de

URL: http://pgp.mit.edu:11371/pks/lookup?op=get&search=0xB9C569CCC8EADFC4
Long-ID: B9C569CCC8EADFC4

Copy-Paste-variant:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: SKS 1.1.4
Comment: Hostname: pgp.mit.edu

mQENBFKaPKUBCACtlCXVZAGV5v0jge/55rksBzq/cWUR0eJNFbolUo9XgUPiNUH8nVOz0K8p
2qS2P6vnWdpwArO6JSCSZTA1IdPC6GVOT2Jn8kxCWopcOB5ODWbZxDb7YY9ZpAvA0qDHSil9
6CzSbVTjHsMRiJqZ6a2F+lY5W4NeWMJtWOCtgLhxiz5wJeQSE3I3LOc/KXqI+eKbgSpXDFTi
cGvxG3rnnXZvvRP9MGP1oGQ7MsVsLzIkE6ruTWJz3pi6ZJhW91W4BnOaEzpu5w5CykJXG9l4
xPfXp50cbh4cj/0ZAZ0jpyNNjF+2pdiHKNKe+wI3HMqLmx1mrpcS17qJM5pERHLJECojABEB
AAG0JVNlYmFzdGlhbiBLcmFqZW5za2kgPHNrQGZyZWVzaGVsbC5kZT6JATgEEwECACIFAlKa
PKUCGwMGCwkIBwMCBhUIAgkKCwQWAgMBAh4BAheAAAoJELnFaczI6t/En6wH/1dF2+/EvWKC
QQTOln9+4JNimxbr9ECXL2/93Bg0zxUrFxUqhIC6154LqS3Ncc/P4dhFGWyr/7Rk3DV3deiT
GKnvX1vgpd6xMhXn1yuMlzDkyIKZCUc5IsrQMf5cBHtENxQEwPn4hje4Az28jKtTaCkPV6ni
nN8eM7Qd8RlW+QbUmg/aqZP7b0MGaJjNAILFFtjx8S7fROJi+/47RxZBxsgZvID1jlWpwZzE
Uqq7sBa7sS13lY/v5gIf7rapk+K6MBakI8dagkUNz5zihI+fLxSedrp2qn5RG9MIDU+Ec92x
dLZADjwowE8lIpXn0IhEPJSw9JLXZCJ6ZI0tLWVG5Wa5AQ0EUpo8pQEIALBXy7oUGN1iAdh3
bC08y+6os4bPf1BqsWB92YsKK9Lc6ZrOfr0I1RerpNBfn9uAlKwyvxtPRkEBe7E6ygWkNEqq
GxZMzDuAmzRQ8xmSoNch4rD09LF2XYHZAEFplhEaXQVn/2hPodUG0hgPxcT4IjvcVwbkabtM
R/qr+cAj5NDlsepNw/KHN7IHu1gR07PqnKSmILEH3+BPNBncZE0TXU60vpLfFs/2wFLZ1NaP
NHX3bW++r001fa0kenHRs5ASvzm1SCXLNuo3xTWjVGgGJ/33MHU7W600ByaRW3evUXJ2ByHy
p3wLSc0oF9RfqZgMcX0IuNHcHem1CVnisELn1nEAEQEAAYkBHwQYAQIACQUCUpo8pQIbDAAK
CRC5xWnMyOrfxGtGB/oDzCiwtySmM9s7T5Ej8EbpsHrLZdjmmpCeL5oit+wyHVgZ6r/P95ti
2Pkfg2FWJCB1C5d/OIXBEr+iWL5mXNqoddkzO7PnHg6JC01dliPazo0FmeMNkG56n51IVPyV
fkSzXlwm4A2eh1DKJfJ1HA/m7riz0Mmd8y/2LihDa3x8huJeCnQt6bCKwsuRI445lEcvY7bg
bP6vLvrloKTZ3pX53+UjGpqi5c+xkn7hmecHnCIJeHouVzCm80DZhWD8HNfoglC7xqrlLfkl
TofiababVtBnH8GBkv2iWMUM8pb+8hZElNYebLy044X9zOoRPmUo0Ym0jfzrYjB4awXGEPqa
=VaYe
-----END PGP PUBLIC KEY BLOCK-----
```

S/MIME - Public Key

If you prefer s/mime, this is the right key. address: sk@ freeshell.de

Download-URL: https://freeshell.de/smime.txt

Copy-Paste-variant:

```
-----BEGIN CERTIFICATE-----
MIIErzCCA5egAwIBAgIQZrRVwxe9sOu13VlGowUlKDANBgkqhkiG9w0BAQsFADBd
MQswCQYDVQQGEwJCRTEZMBcGA1UEChMQR2xvYmFsU2lnbiBudi1zYTEzMDEGA1UE
AxMqR2xvYmFsU2lnbiBQZXJzb25hbFNpZ24gMSBDQSAtIFNIQTI1NiAtIEcyMB4X
DTE0MDUzMDE0NDMxNloXDTE3MDUzMDE0NDMxNlowOjEYMBYGA1UEAwwPc2tAZnJl
ZXNoZWxsLmRlMR4wHAYJKoZIhvcNAQkBFg9za0BmcmVlc2hlbGwuZGUwggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB++yJoWokc6ui9TSqSZ/+OS83FKal
FXIWuK1Mw4yN3MKiSt3VUke7qRXbnyMth6WrN9WcvoSs+0/NnpiRBwmjgtuTFOd3
WDlnz/Ni8J9JfplbvdPwjyl1YH42MBU5WmcV3ZQ4AruXxjWwSISn2Qy6GlDLszKB
cddUlq4y5MhPQUdEayprhmmmllKZCIQK1YJ+B3RUdBxGUvcCrZ8Jj6vgC+4dbX33
C/E9NxhiLewqZY/Me5YHfVf7gL+CLuNyo4HNaFTKtn4DY9D6XUy+q0rzCD1c/H/O
71EW7HvTR891fBb498OWDjBqgPIV9FiqpzddpXHc1hwk1DVIKQ1se/PdAgMBAAGj
ggGMMIIBiDAOBgNVHQ8BAf8EBAMCBaAwTAYDVR0gBEUwQzBBBgkrBgEEAaAyASgw
NDAyBggrBgEFBQcCARYmaHR0cHM6Ly93d3cuZ2xvYmFsc2lnbi5jb20vcmVwb3Np
dG9yeS8wGgYDVR0RBBMwEYEPc2tAZnJlZXNoZWxsLmRlMAkGA1UdEwQCMAAwHQYD
VR0lBBYwFAYIKwYBBQUHAwIGCCsGAQUFBwMEMEcGA1UdHwRAMD4wPKA6oDiGNmh0
dHA6Ly9jcmwuZ2xvYmFsc2lnbi5jb20vZ3MvZ3NwZXJzb25hbHNpZ24xc2hhMmcy
LmNybDBZBggrBgEFBQcBAQRNMEswSQYIKwYBBQUHMAKGPWh0dHA6Ly9zZWN1cmUu
Z2xvYmFsc2lnbi5jb20vY2FjZXJ0L2dzcGVyc29uYWxzaWduMXNoYTJnMi5jcnQw
HQYDVR0OBBYEFPmW20op7NINlKE6zT3zQ+LwJIL9MB8GA1UdIwQYMBaAFP4pqbj/
nFvJ7ULZbnfYNFdBp20FMA0GCSqGSIb3DQEBCwUAA4IBAQBpmSlGxcutBHIb28sk
XdF9I1x342jPMIYmsDNVs0XulKe2gVhGngsD9NO9cWrk8zbc0j+jVb+U3PzopMuc
id5m9X8ti2UOAzyjNNm67QXjsN++oQxcUIBmGm38xfAC51Oaqfo0U9AUr6LVlMQd
owHC5/7hfsXgblZ2q/OZeXnNGVnekcOalS5VPlAn1kYov87k9Vofw4TBfRMGTbNz
sdkLlVWbZ4FHYypnxtAiGuuC4oHB0fV3pnQqalBaGCi5NFObfFouQOM0867s06pP
YPo4eQGL77j0HCSqz7TA5AOw/+7zA5KXIQuQVylBvl9RcijysAc5IluEdVqd/QYy
Idzo
-----END CERTIFICATE-----
```

Authentication and access

SSH

OpenSSH server here accepts connections to “freeshell.de” on the default port (TCP/22) for interactive sessions. With Linux and MacOS I recommend you “ssh” on the terminal. With MS Windows “putty” is the favoured client:
http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html
When you connect from a computer for the first time, please always check the fingerprint!

Password

Your first login will be password-based. After that, there are a couple of possible enhancements or variants:

Public Key

You already have a public key identity for SSH (type: RSA or ED25519) ? Just fill **$HOME/.ssh/authorized_keys**

…with your public key, to login with a keyfile in the future. In case you don't have a look here:
https://help.ubuntu.com/community/SSH/OpenSSH/Keys

If you additionaly like to improve the SSH secrecy I recommend this article:
https://stribika.github.io/2015/01/04/secure-secure-shell.html

Hint: File transfer to the server is only possible using SFTP or SCP. Classic (unencrypted) FTP is **not** possible anymore.

Yubikey

URL: https://www.yubico.com/products/

Another possibility to login is the "Yubikey". It's basically a USB-Device that emulates a keyboard. It generates throw-away one-time-passwords. Set it up like this:
$ **cd $HOME**
$ mkdir .yubico
$ cd .yubico
$ cat >authorized_yubikeys
<activate your yubikey by pressing the sensor>
<Ctrl-D>

Now take a text-editor and modify the file according to this schema:
yourlogin:first_12_chars_of_yubi_output

The first 12 chars are the public identity of your key. Just remove anything beyond char 12.

Example result after editing:
psmith:ccclksjehdzu

Two-Factor-Login (forced)

You'd like to be forced to use two ways of authentication when logging into the system? Just use the homepage request form and tell me about that. I'll then add you to the "Force Two-Factor"-Group.

The login procedure is then the following:
- Login with SSH-Public-Key (must!)
- Then you'll see:

Authenticated with partial success.
Password:

Here you now have two possibilities: Enter your normal text-based password **OR** hit the yubikey!

The server-side setup of that part by the way looks like this in sshd_config:

...

Match Group mfagroup

    AuthenticationMethods publickey,keyboard-interactive

...

OTP / OPIE Auth

URL: https://en.wikipedia.org/wiki/OPIE_Authentication_System
And there is also OTP/OPIE available here. Technically comparable to the yubi-variant. You generate one-time-passwords, which in this case are typed into the keyboard. No special hardware needed.

$ opiepasswd -c -f

Now you're asked for a at least 10 digit passphase, the output looks like this:

ID yourlogin OTP key is 499 fr0761
TEN BILE MAID BARE SICK ABE

What does that mean?
“499” is the sequence nu,ber
“fr0761” is the “seed”, so to say the initializing vector for your OTPs.

Now for the client-side. You need a piece of software to generate the passwords. In case of some older Debian you install the package “opie-client”. Usage goes like this:

Terminal 1
$ ssh you@freeshell.de
Password: (ENTER)
Yubikey for... (ENTER)
otp-md5 497 fr0761 ext, Response:

In another terminal window you prepare your one-time-password:

Terminal 2
$ opiekey 497 fr0761

Now after entering your passphrase you are provided with the OTP for login:
WALK NEWS NE COAL MUFF BEAD

Hint: You can generate some OTPs in advance!
Example:
$ opiekey -n 10 497 fr0761
(generates the next 10 valid OTPs)

limited access / censored internet

So you are limited in some way regarding your internet connection. It's still likely that you can connect anyway. Let me show you some alternative ways to get into the system. Use an alternative port:

$ ssh ssh.freeshell.de -p443
$ ssh work.ham.to -p443 (same IP, but more unsuspicous name)

If your only limitation is not being able to run SSH-client software use the browser variant:
https://gateone.freeshell.de

If all else fails, use **DNS2TCP.**
If you have access to a linux machine install the package “dns2tcp”.

With this method the TCP-packets for SSH are sent out covered in "normal" DNS-requests.

Usage:

Terminal 1 (start the tunnel / program)
$ dns2tcpc -z tcp.ham.to dns.ham.to -l 12345 -r ssh
(Tunnels SSH through DNS and port-forwards freeshell-SSH to localhost:12345)

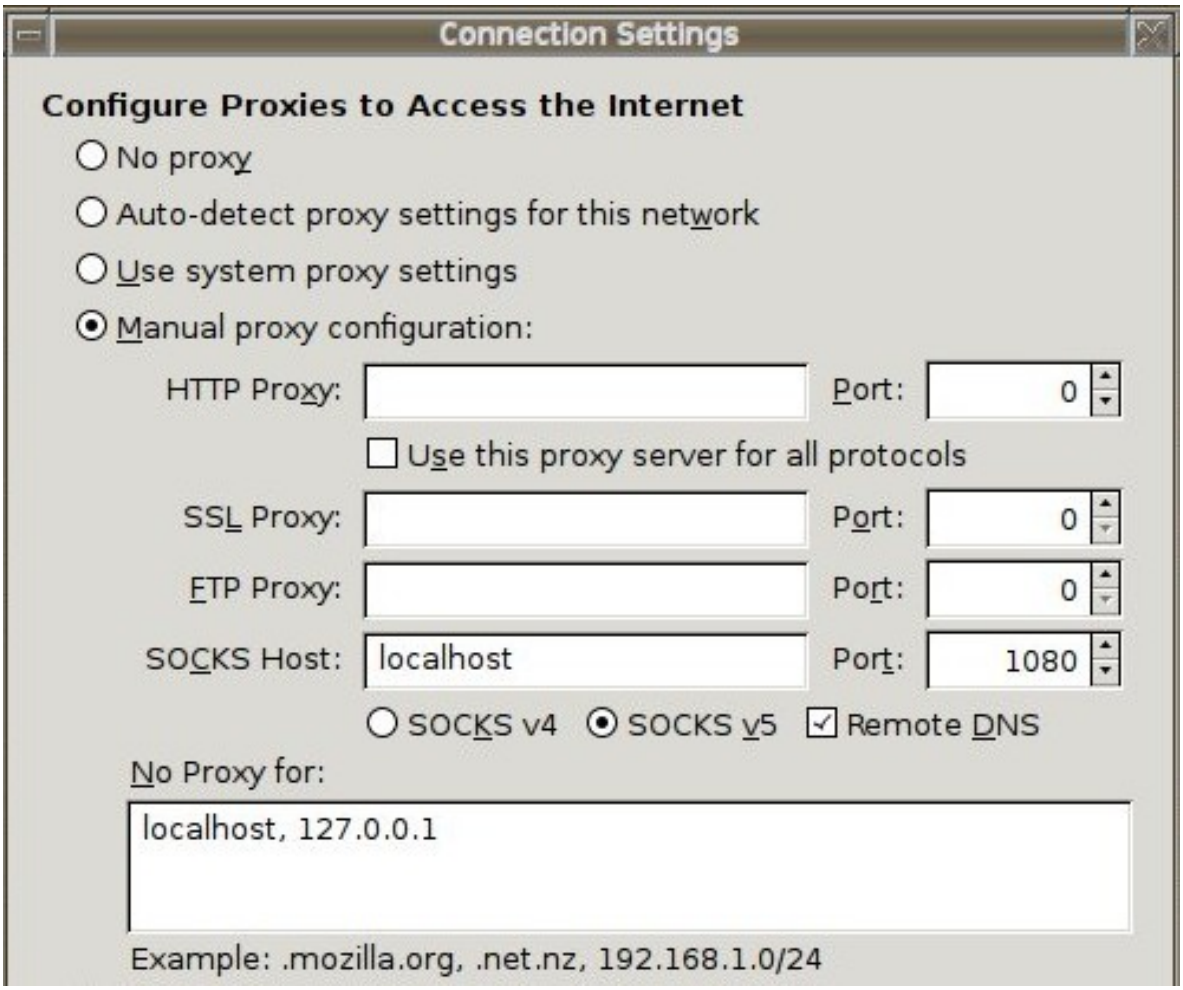
Terminal 2 (login to freeshell)
$ ssh your_freeshell_login@localhost -p12345

In case you not only want to login to the shell but like to proxy-surf through that connection:

$ ssh -o “CompressionLevel=5” -C -4 -ND localhost:1080 you@localhost -p12345

Now you got yourself a socks-proxy to freeshell.
Hint: You won't get a shell prompt with that command, that's normal.

This is how to setup e.g. your firefox to use that proxy safely:



It's imperative to check the “Remote DNS” box. Otherwise your "evil" ISPs DNS might get a clue to where you surf.

This method in general will be really slow because of the DNS2TCP overhead in general.

Hint: Anyway, even if you can connect to freeshell without hazzle, you are welcome to use the socks-proxy-technique as well.

Software and services

OS

The server runs Debian 7 (Wheezy) 64-Bit-version. In irrgeluar intervals the distribution gets updated the the latest "stable" release. There are 3rd-party software-dependencies that normally lead to 3-4 months of delay until I'm able to upgrade (after initial release). Please be patient.

Installation of additional packages

In case you miss a package just ask for it using the request form on the homepage. I will install almost any package that is available to official channels (in respect to the running release) :
https://www.debian.org/distrib/packages
http://backports.debian.org/Packages/

Firewall

This system uses a packet-filtering "iptables"-firewall. All ports (from the outside) to non-standard services are closed. In case you need a private port please let me know through the request form on the homepage.

Mailsystem

Postfix

The MTA on the server is postfix. The following services are configured.

Servername: freeshell.de
Port 25 (SMTP) sending email (Relaying) with auth. STARTTLS (forced)
Port 587 (Submission) sending email with auth. TLS (forced)
Port 465 (SMTPS) sending email with auth. TLS (forced)

The mailbox-format used on the system is “Maildir”. So your email resides in:
$HOME/Maildir/ (...)

Domain names
You are reachable with the following addresses:
you@freeshell.de (primary)
secondary: @freeshell.ch, @freeshell.at, @nic-nac-project.de
More domain names may follow.

Anti-Spam / Anti-Virus

Email on the system is passed through a couple of techniques (in- and out)

- ips.backscatterer.org in “safe mode”
- policyd-spf (freeshell.de uses “hard fail” = strict in its own DNS entries)
- policyd-weightd (RBL-list checks)
- DKIM check (OpenDKIM in “safe mode” receiving side, otherwise mailing-lists would break)
- BATV (you get automated BATV-envelope-adresses to your sent mails)
- ESET-Antivirus check (this commercial AV checks for malware and trojans)

Hint: Maximum element size (per mail element) is 50MB.

Dovecot - Receive mail

Dovecot provides your mailbox through **POP3** and **IMAP** on the following ports:

Servername: **freeshell.de**
Port 110 (POP3) STARTTLS (forced)
Port 143 (IMAP) STARTTLS (forced)
Port 995 (POP3S) TLS
Port 993 (IMAPS) TLS

On the shell you can run preconfigured “mutt” or “pine” to access your mailbox.

There are also webinterfaces in place:

URL: https://secure.freeshell.de/squirrelmail/src/login.php
SquirrelMail. Type: spartanic and functional

URL: https://freeshell.de/rc/
RoundCube. Type: modern and good looking

Zarafa - Groupware

URL: http://www.zarafa.com

In case you want full collaboration experience and simple email is not enough for you. Zarafa is a AGPL3 groupware solution that provides (besides basic email services) things like:

- Calendaring (also via ActiveSync aka “Exchange-Mailbox”, see below)
- Tasks
- Notes
- Contacts (address books)

Zarafa is in permanent co-existence with the "normal" mail-system. On the shell you can at any time migrate to Zarafa.
$ **move-in.sh** moves your current mail to into the zarafa-mailbox using "imapsync" in the background.

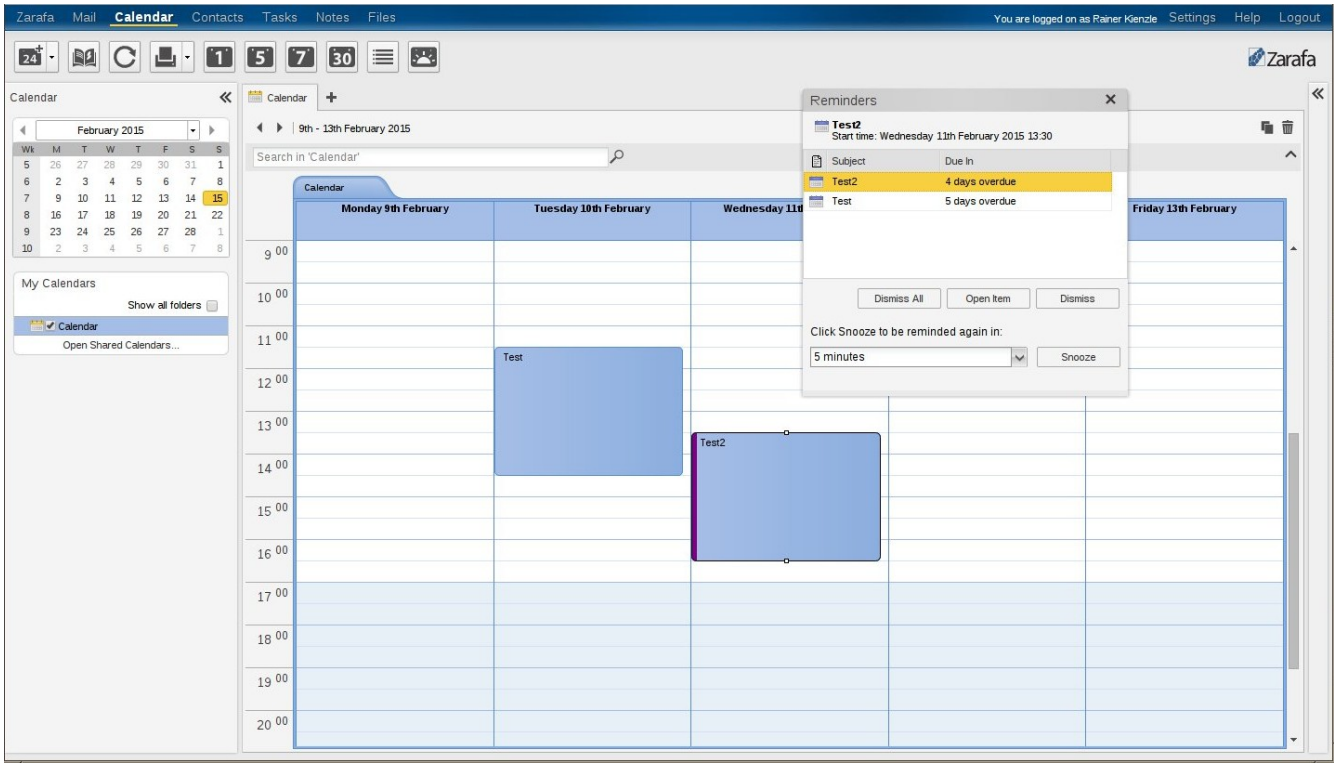
In case you just want to look around without migrating for real you can login into e.g. Zarafa WebApp anyway. The account is automatically in existence, just unused (empty).

Classic IMAP or POP to the zarafa account works as follows:
Servername: **zarafa.freeshell.de**
- Port 995 (POP3S) TLS
- Port 993 (IMAPS) TLS

Sending email (SMTP) with a mailclient of your choice:
Not different from the normal Dovecot-system, SMTP is simply the same.
Servername: **freeshell.de**

Visit this URL for the groupware web-client "Zarafa WebApp"
URL: https://secure.freeshell.de/

(Please zoom in with your PDF viewer to see details.)



Of course there is always a way back. In case the zarafa account doesn't fit your needs:
Just delete your $HOME/**.forward** file.
Now, new mail will arrive in your classic "Maildir/- dovecot-mailbox" again.
Mail from the zarafa account can be moved back using a mailclient of your choice.

ActiveSync – Push-Services

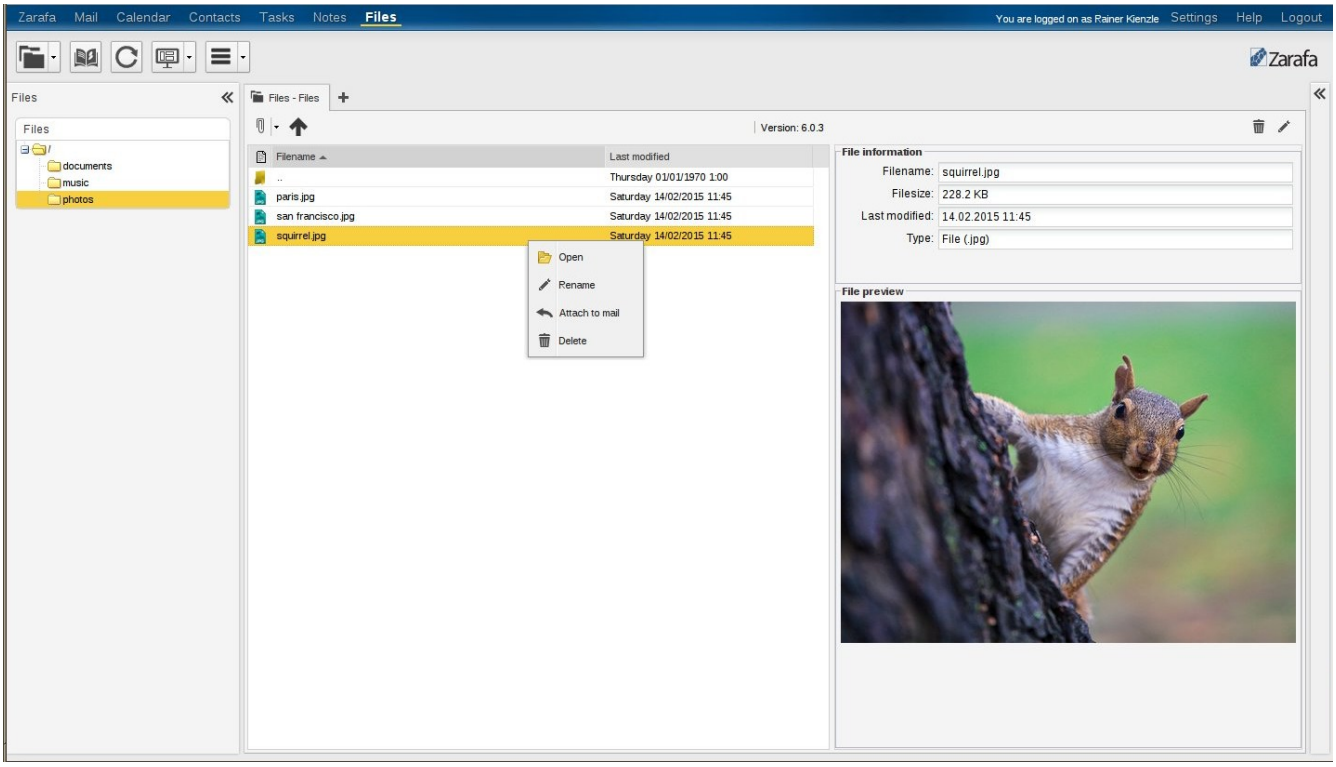
In case you use your zarafa account, you can configure your mobile devices to sync with it. Choose “Exchange account" and sync contacts, tasks, calendar and mail with it.

Servername: **freeshell.de**
Login and password as always.
Domain field: (leave empty)

Owncloud

URL: https://freeshell.de/owncloud/
Your account here is automatically equipped with some local owncloud storage. It's usable by browser or the native client. By the way: I only support the file-sharing features. All other fancy owncloud-features are officially unsupported by me.

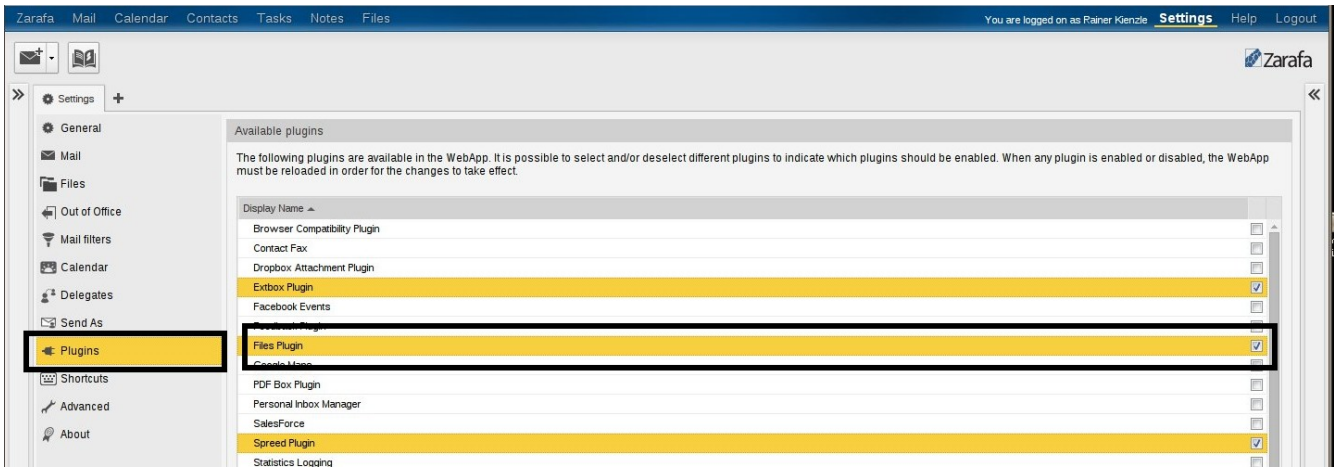
You can also configure your Zarafa Webapp to automatically use your owncloud storage:



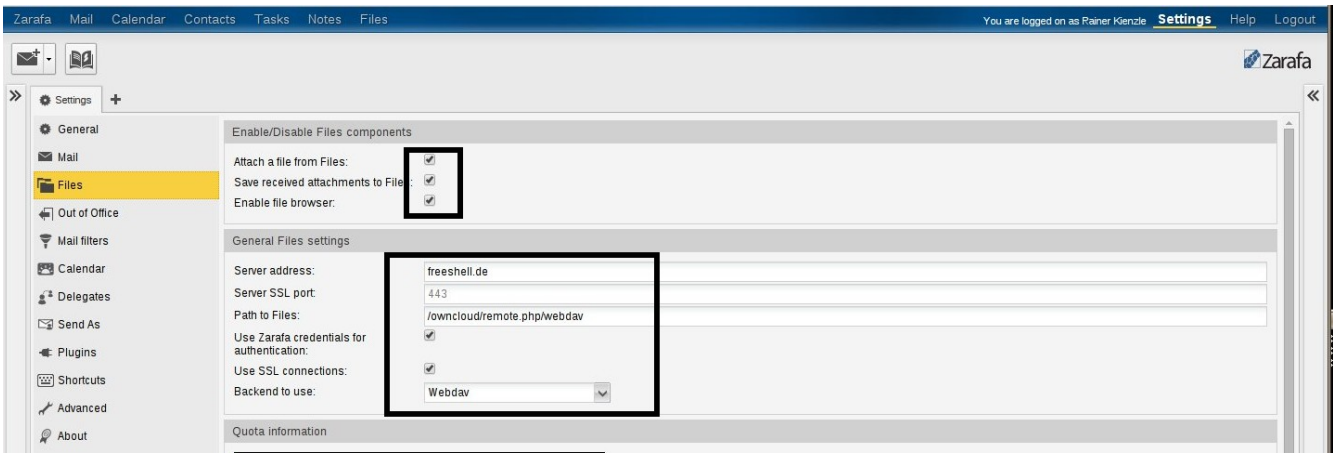
In case the "Files"-feature in Zarafa-WebApp is not automatically enabled, here is how to do it:

- Login to Zarafa WebApp: https://secure.freeshell.de/

(Please zoom in with your PDF viewer to be able to read the instruction details.)



After that login/logoff **twice** and head back for the "Settings":



After that login/logoff **twice** again. Now owncloud storage is usable in your zarafa groupware account as well. Have fun.

Homepage / PHP

Your account automatically provides a directory where you can publish your homepage. The URL is as follows:
http://freeshell.de/~yourlogin/
...which by the way gets automatically redirected to: **https://freeshell.de/~yourlogin/**

To put content into it that should be reachable from the outside, put it into this directory:
$HOME/public_html/
This is so to say your documentroot.

Script languages:
PHP 5.4.xx is installed and available, Perl and Python as well.

MySQL-Database

In case you also need a mysql database, just ask using the request form on the homepage.
PHPMyAdmin is installed here: https://secure.freeshell.de/phpmyadmin/

Tor and anonymous surfing

This project supports and promotes anonymous surfing. “Tor” is installed and running in the server. It is accessible through the local privoxy-proxy servuce as well as with “tsocks”. Set the proxy variables as follows:

$ export http_proxy=”http://127.0.0.1:8118”
$ export https_proxy=”http://127.0.0.1:8118”
Privoxy of course keeps no log files here.

Here is an example for "tsocks" usage:
$ tsocks ssh login@where_ever.com

Support and help

In case of difficulties that are not covered by the manual please leave me a message through the request form on the homepage. In case the issue requires that: Write me an encrypted email.

Hint: Most login problems derive from “**fail2ban**” here. The server blocks any attempts to the system from your source-IP when a attempted login fails 5 times in a row. The block lasts 1 hour. This slows down brute-force-attacks and is in place to protect your account.

Link collection

Links to provided "freeshell.de" services
- HTML5-SSH-Client: https://gateone.freeshell.de/
- SquirrelMail Webmail: https://secure.freeshell.de/squirrelmail/
- Roundcube Webmail: https://freeshell.de/rc/
- PHPMyadmin: https://secure.freeshell.de/phpmyadmin/
- Zarafa WebApp: https://secure.freeshell.de/
- Etherpad Textcollaboration: https://etherpad.freeshell.de:9002/

External useful links
- Mailserver-Crypto check: https://ssl-tools.net/mailservers
- Webserver-Crypto check: https://www.ssllabs.com/
- “Tails” Privacy-Live-Distro: https://tails.boum.org/
- DANE-SMTP-Validator: https://dane.sys4.de/
- DNSSEC-Zone-Analyzer: http://dnssec-debugger.verisignlabs.com/
- DNSSEC-Browser-Plugin: https://www.dnssec-validator.cz/
- Secure E-Mail Test Tools: http://checktls.com/
- Meta-RBL-Check-Seite: http://multirbl.valli.org/
- Test-Mailaddress for various Checks: test@allaboutspam.com
- Test-Mailaddress for various Checks: check-auth@verifier.port25.com

Disclaimer / Misc.

The terms and conditions as well as the data protection statement are available through the homepage www.freeshell.de on menu item "Contact".

All documents are updated regularly. Please make sure you always use the most recent version.

Remember, this is a “shared system”. Over 2000 people from literally all over the world share the server. Please treat persons with respect and use the available resources wisely.